



**TURUN AMMATTIKORKEAKOULU**  
**ÅBO YRKESHÖGSKOLA**

**Kai Kolima**

**WLAN TURUN AMK:n**  
**LEMMINKÄISENKADUN TOIMIPISTEESSÄ**

**TIETOJENKÄSITTELY**  
**TURKU**  
**Kevät 2010**

|  |                                      |
|--|--------------------------------------|
| TURUN AMMATTIKORKEAKOULU   | Koulutusohjelma<br>Tietojenkäsittely |
| Tekijä<br>Kai Kolima   |                                      |
| Työn nimi<br>WLAN TURUN AMK:n<br>LEMMINKÄISENKADUN TOIMIPISTEESSÄ  |                                      |
| Suuntautumisvaihtoehto<br>Tietoliikenne  | Ohjaaja<br>Esko Vainikka             |
| Aika<br>Toukokuu 2010  | Sivumäärä<br>36 sivua + 1 liite      |
| <p>Kipinä tähän opinnäytetyöhön lähti alun perin opiskelijoiden negatiivisesta palautteesta Lemminkäisenkadun langattoman lähiverkon toimintaan kannettavilla tietojenkäsittelylaitteilla. Asian pintapuolisen selvityksen jälkeen kävi ilmi, että Lemminkäisenkadun langaton lähiverkko on Masterplanet –yrityksen tuottama, osa maailman laajinta langatonta lähiverkkoa SparkNetiä. Ilmeni myös ettei kyseisestä verkkoratkaisusta ole olemassa minkäänlaisia dokumentaatioita. Opinnäytetyön aihe oli siis suoraviivainen: kartoittaa tukiasemat, kuuluvuus ja toiminnallisuus sekä dokumentoida kaikki em. ominaisuudet.</p> <p>Opinnäytetyön rakenne on varsin suoraviivainen ja se jakautuu kahteen osaan. Ensin käsitellään teoreettisella tasolla tietoliikenteen perusteita alkaen aina OSI:n ISO-mallista ja lopulta päädytään tulevaisuuden kehityskohteisiin mm. hajaspektritekniikan osalta. Kattavan teoreettisen osion jälkeen muunnetaan soveltuva teoria käytäntöön ja ryhdytään analysoimaan Lemminkäisenkadun langatonta lähiverkkoratkaisua passiivianalysaattorien avulla. Toissijainen tavoite oli muodostaa opinnäytetyö niin, että kuka tahansa voisi tulkita ja ammentaa tietoa siitä. Tätä tavoitetta on tuettu mm. sanasto-liitteellä.</p> <p>Koko empiriaosuus, eli mittausmenetelmät, pisteet, laitteisto ja mikä oleellisin tulokset on julistettu määrättömäksi ajaksi salaisiksi, joten niitä ei voi käsitellä tämän tiivistelmän puitteissa.</p> |                                      |
| Luottamuksellinen: Koko empiria, määrittelemätön aika  |                                      |
| Hakusanat: WLAN, SparkNET, langaton lähiverkko, kiinteistöverkot   |                                      |
| Säilytyspaikka: Turun ammattikorkeakoulun kirjasto. Lemminkäisenkatu.  |                                      |

|  |  |  |
|--|--|--|
| TURKU UNIVERSITY OF APPLIED SCIENCES   |  | Degree Programme<br>Information Technology |
| Author<br>Kai Kolima   |  |  |
| Title<br>WLAN at Turku University of Applied Sciences, Lemminkäisenkatu  |  |  |
| Specialization line<br>Data Communication  | Instructor<br>Esko Vainikka                    |  |
| Date<br>May 2010   | Total number of pages<br>36 pages + 1 appendix |  |
| <p>The spark to do this final thesis originally started from the author's personal frustration towards the WLAN network at Lemminkäisenkatu using portable computing devices. After doing some research it was discovered that the WLAN is produced by the company Masterplanet, and it is a part of the largest WLAN in the world, Spark-Net. It was also found out that there is zero documentation on the network. So that meant my thesis topic was clear: to map the access points, their broadcast radius and functionality, and document everything.</p> <p>The structure of the thesis is very simple and it is split into two distinct parts. First the theoretical part researches the fundamentals of data traffic starting from the OSI ISO model and ending up with future development ideas such as wide spectrum technology. After the comprehensive theoretic part, the suitable parts of theory are taken and implement it to the real world by analyzing the WLAN network at Lemminkäisenkatu with passive analyzer devices and software. A secondary goal for this thesis was to make it simple enough for everyone to be able to interpret and use it for their own purposes. To make this easier I tried to simplify it with for example the vocabulary appendix.</p> <p>The entire practical part of the work, including measurements, equipment and most importantly the results have been declared classified, so I can not use them in this abstract.</p> |  |  |
| Confidentiality status: Entire empiric part, unspecified amount of time  |  |  |
| Keywords: WLAN, SparkNet, Wireless local area network, office network  |  |  |
| Deposit at : Turku University of Applied Sciences library. Lemminkäisenkatu.   |  |  |

# **SISÄLTÖ**

|  |    |
|--|----|
| <b>1 JOHDANTO</b>  | 6  |
| <b>2 WLAN PERUSTEET JA STANDARDIT</b>                      | 8  |
| 2.1 ISO:n OSI -malli                                       | 8  |
| 2.2 TCP/IP   | 10 |
| 2.3 Lähiverkon konsepti                                    | 11 |
| 2.4 Ethernet 802.3   | 14 |
| 2.5 Langaton siirtotie lähiverkossa                        | 17 |
| 2.6 WLAN, sijoittuminen OSI-malliin                        | 20 |
| 2.7 IEEE 802.11  | 23 |
| <b>3 KÄYTÄNNÖN SOVELLUKSET</b>                             | 24 |
| 3.1 Wi-Fi  | 24 |
| 3.2 Standardit a-n   | 24 |
| 3.3 Langattoman verkon keskeiset laitteet                  | 27 |
| 3.4 Tukiaseman kuuluvuus                                   | 29 |
| 3.5 Siirtotien häiriön lähteet                             | 30 |
| 3.6 Langattoman siirtotien suojaus                         | 31 |
| <b>4 LEMMINKÄISENKADUN TOIMIPISTEEN ESITTELY (Salattu)</b> |    |
| <b>5 LANGATTOMAN VERKON DOKUMENTOINTI (Salattu)</b>        |    |
| <b>6 POHDINTA</b>  | 35 |
| <b>LÄHTEET</b>   | 36 |

## **LIITTEET**

### **1 Sanasto**

## **KUVIOT**

|  |    |
|--|----|
| Kuvio 1. ISO-mallin ja TCP/IP-protokollan vertailu         | 9  |
| Kuvio 2. TCP ja IP -protokollien välinen suhde             | 11 |
| Kuvio 3. Lähiverkkotopologiat                              | 14 |
| Kuvio 4. Ethernet  | 15 |
| Kuvio 5. Monta tukiasemaa samassa virtuaali-LAN:ssa        | 18 |
| Kuvio 6. Ad-hoc ja infrastruktuuri –verkkojen väliset erot | 20 |
| Kuvio 7. OSI-malli   | 22 |
| Kuvio 8. WLAN-standardit                                   | 23 |
| Kuvio 9. Attenuaation lähteet                              | 30 |

# 1 JOHDANTO

Langattomat lähiverkot alkavat olla arkipäivää jo organisaatiossa kuin organisaatiossa. Turun ammattikorkeakoulun Lemminkäisenkadun toimipiste ei ole poikkeus langattomien verkkojen käyttäjänä, ja miksi olisi? Jokaisessa kannettavassa multimediapöytätelaitteessa, oli kyseessä sitten kännykkä tai kannettava tietokone, on nykyisin langattoman lähiverkon tarvitsemat toiminnallisuudet kiinteinä varusteina. Opiskelijoilla nämä em. multimediapöydät ovat myös tavattoman yleisiä opiskeluapuvälineitä, sillä niiden hankkiminen ei ole enää varsinaisesti mikään kustannuskysymys ja niiden tuottama hyöty opiskeluun on huomattava.

Oppitunneilla opiskelijat voi hakea lisätietoa verkon avulla parhaillaan läpi käytävästä asiasta, verkostoitua hyppytuntien aikana käyttäen Web 2.0-palveluja tai vaikka tarkastaa ilmoitukset verkko-oppimisjärjestelmästä. Tämän kaiken Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteessä mahdollistaa kätevästi langaton lähiverkko nimeltä SparkNet, joka on maksutta opiskelijoiden ja muun henkilökunnan käytössä mihin kellonaikaan tahansa ilman näkyviä verkkokaapeliratkaisuja.

Tämän opinnäytetyöni tarkoituksena on aluksi luoda kattava teoreettinen kuvaus ja pohja mistä langattomassa lähiverkossa yleensäkin on kyse. Esittelyssä on OSI-malli ja IEEE:n 802.11-standardi laajennuksineen. Vahvan teoriapohjan jälkeen ryhdyn esittelemään miten teoria on muutettu käytännöksi Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteessä.

Lisäksi esittelen verkon mittaustulosten perusteella ehdotuksia verkon parantamiseksi. Otan myös kantaa käytettävyyden ja tietoturvan toteutukseen. Kaikki parannusehdotukset suhteutetaan käytössä olevan kiinteistön asettamiin haasteisiin ja keskimääräisen käyttäjäkunnan tarpeisiin.

Analysoin myös yksityiskohtaisesti verkon kulmakivinä toimivia tukiasemia ja otan kantaa niiden sijoitukseen ja yleiseen toiminnallisuuteen. Dokumentoin myös niissä

käytetyt asetukset, jotta uusien verkkolaitteiden käyttöönotto sujuisi mahdollisimman mutkattomasti ylläpitohenkilöltä.

Esittelen myös pintapuolisesti langattoman järjestelmän taustalla toimivan käyttäjän autentikaation nimeltä FreeRadius, joka on maailman yleisin käyttäjäautentikaatioon tarkoitettu ohjelmisto. FreeRadius mahdollistaa omalta osaltaan SparkNetin mutkattoman käytön myös Lemminkäisenkadun toimipisteen ulkopuolella samoilla tutuilla tunnuksilla, joita opiskelija käyttää Lemminkäisenkadun Windows-verkossakin.

Oma kipinä ryhtyä tutkimaan Lemminkäisenkadun toimipisteen langatonta lähiverkkoa syntyi lähinnä sitä kautta, että aktiiviopiskelija-aikanani käytin kyseistä verkkoratkaisua lähes päivittäin koulutoimieni suorittamiseen. Vuosina 2006-2009 verkon toimivuus oli vähintäänkin kyseenalaista, joten 99.999 % saatavuus tuskin täyttyi. Maailman johtavin verkkolaitteiden valmistaja (Wikipedia 2010b, [viitattu 25.2.2010]) Cisco Systems käyttää viiden yhdeksikön sääntöä mittatikkuna, kun määritellään teleoperaattoritason verkkoja, eli verkon pitäisi olla käyttäjien saavutettavissa 99.999 % ajasta (Wikipedia 2010a, [viitattu 25.2.2010]) Suurimmat ongelmakohdat esiintyivät juuri verkon saatavuudessa. Esimerkiksi niinkin oleellinen asia kuin tukiasemien fyysinen sijainti oli mysteeri verkon ylläpidolle. Turun AMK:n IT-henkilöstö on myös raportoinut minulle, että edes suppealla SparkNet-dokumentilla olisi suurtakin kysyntää, koska tätä opinnäytetyötä tilattaessa ei langattoman verkon nykytilasta ollut kennelläkään minkäänlaista kuvaa.

Opinnäytetyön tuloksena syntyy AMK:n IT-henkilöstölle kattava kuva Lemminkäisen kadun langattomasta verkosta, jossa on sekä tukiasemien sijainnit, tukiasemien keskimääräinen kuuluvuus keskeisissä opetustiloissa, verkon fyysinen rakenne eli missä tukiasemat sijaitsevat sekä miten ne liittyvät SparkNetin kautta lopulta Internetiin. Toimeksiantajana työssä toimii tietoliikenteen yliopettaja Esko Vainikka.

## 2 WLAN PERUSTEET JA STANDARDIT

### 2.1 ISO:n OSI-malli

Open systems interconnection (OSI, avoimien järjestelmien yhteenliittymä) on teoreettinen referenssimalli, jonka kehitti Organization for Standardization eli ISO. ISO ei ole akronyymi vaan sana on johdettu kreikan kielen sanasta isos, joka tarkoittaa yhdenmukaista. OSI on suunniteltu malliksi tietokoneprotokollan arkkitehtuurille sekä kehykseksi protokollien standardien kehitykselle (Stallings 2007, 42.)

OSI-malli on seitsemänportainen, jossa ylemmillä portailla olevat palvelut perustuvat niitä alemmilla portailla olevien tasojen tuottamille palveluille (Petri 2009, [viitattu 25.2.2010]). Joissain tapauksissa teoreettiseen viitekehykseen lisätään vielä teoreettinen käyttäjä, sillä niin kauan kun käyttäjä ei tuota pyyntöjä, järjestelmä on käyttämätön ja käyttämätön järjestelmä on hyödytön.

8. [Käyttäjä]

7. Sovellus (Application). HTTP, FTP, SMTP. Tarjoaa pääsyn OSI-ympäristöön käyttäjille ja toimii rajapintana koko palveluun.

6. Esitystapakerros (Presentation). GIF, JPG, MPEG. On yksinkertaistetusti OSI-mallissa liikkuvan tiedon kielioppi ja samalla erittelee protokollassa liikkuvan tiedon ohjelmaprosesseista.

5. Istuntokerros (Session). SMB, Winsock. Tarjoaa hallintajärjestelmän kahden eri sovelluksen kommunikaatioon. Hallinnoi ja tarvittaessa terminoi yhteyksiä (istuntoja) kahden yhteyksissä olevan sovelluksen välillä.

4. Kuljetuskerros (Transport). TCP, UDP. Tuottaa luotettavan tiedonvälityskanavan kahden pisteen välillä (end-to-end connectivity). Lisäksi se toimittaa palvelut, jotka ottavat kantaa virheistä palautumiseen ja vuon hallintaan tiedonsiirrossa.

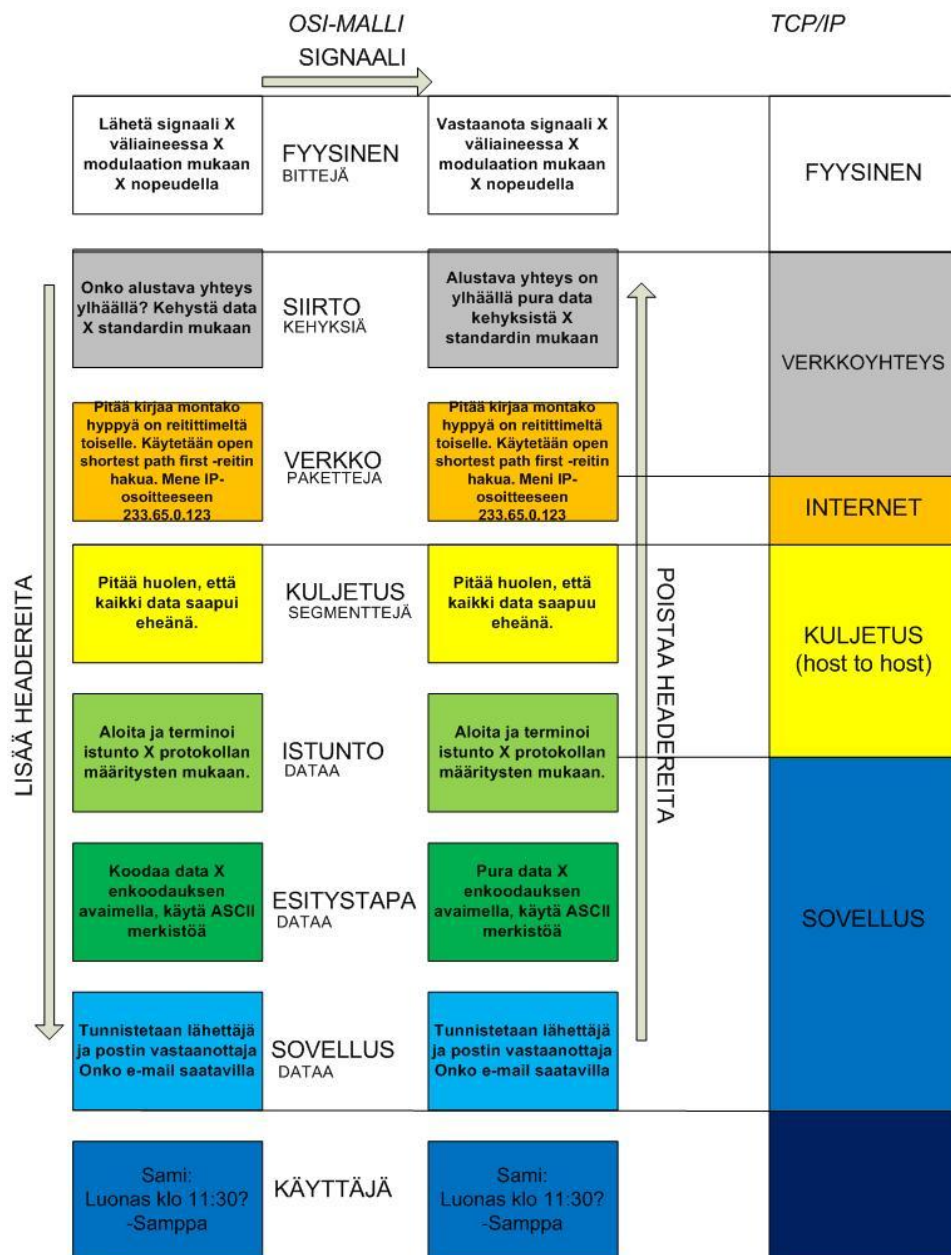
3. Verkkokerros (Network). IP, IPX. Toimittaa ylemmille kerroksille mahdollisuuden olla välittämättä tietoliikenteestä ja kytkemisestä.

2. Siirtokerros (Datalink). ATM, Ethernet. Antaa luotettavan tiedonsiirron läpi fyysisen linkin. Lähettää blokkeja (kehyksiä), jotka tarpeen mukaan synkronisoidaan. Tarkkailee virheitä ja ottaa myös kantaa vuon hallintaan.



1. Fyysinen (Physical). Token ring, Ethernet. Ottaa kantaa ainoastaan rakenteettoman bittivirran lähetykseen väliaineen yli eli on yhteyksissä mekaaniseen tai sähköiseen toiminnallisuuteen. (Stallings 2007, 43.)

Vaikka monia käytössä olevia protokollia on kehitetty OSI-mallin pohjalta, ei esitetty seitsemänportainen malli ole sellaisenaan missään käytössä. TCP/IP-protokollapari on tietoliikenteessä käytetyin ja sillä on vahvat juuret OSI-mallissa, kuten kuvioista 1 voi havaita.



Kuvio 1. ISO-mallin ja TCP/IP-protokollan vertailu (Stallings 2007, 44).

On olemassa lukuisia syitä, miksi TCP/IP on hallitseva arkkitehtuurinen ratkaisu tietoliikenteessä. Suurin niistä on TCP/IP-protokollaparin valmiusaste ja kypsyys aikana, jolloin OSI-protokollat olivat vielä piirustuspöydällä. Samaan aikaan lukuisat liikeyritykset tiedostivat tarpeen interoperatiivisuuteen yli tietoverkkojen. Samoina hetkinä oli vain TCP/IP valmiina todelliseen toimintaan. Toinen painava syy OSI-mallin käytännön hylkäämiseen oli ja on vieläkin tarpeettoman monimutkainen rakenne, joka käyttää seitsemää kerrosta siihen, mihin TCP/IP kykenee vain viidellä (Stallings 2007, 43.)

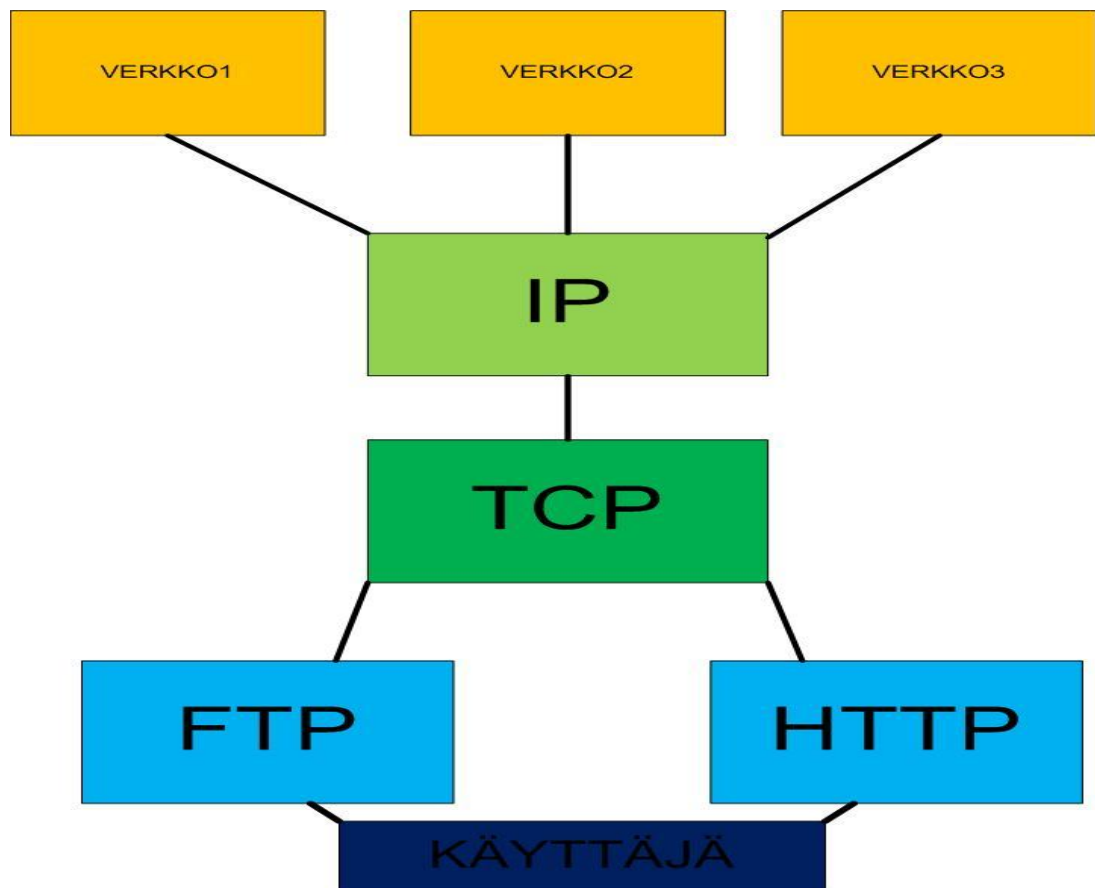
## **2.2 TCP/IP**

TCP/IP on Internet-arkkitehtuuri, joka saa nimensä kahden siihen liittyvän protokollan mukaan. Internet-arkkitehtuuri kehittyi kokeiluista varhaisen pakettikytkentäisen verkon, ARPANETin parissa. Internet ja ARPANET olivat jo olemassa ennen OSI-mallia. Käyttökokemukset, jotka ammennettiin niiden rakentamisesta, antoivat suuria vaikutteita OSI-viitemalliin (Peterson & Davie 2000, 38).

Internet Protokolla eli IP on määritelty tarkemmin IETF RFC791 dokumentissa. Tämä protokolla tukee eri verkkoteknologioiden yhdistämistä yhdeksi loogiseksi interverkoksi eli lähiverkkojen kokonaisuudeksi. Tämä ottaa kantaa reitityskerroksen datagrammipalveluun TCP/IP-arkkitehtuurissa (Protocols 2010, [viitattu 29.1.2010].) IP-kehyksen otsikko sisältää reititystietoa ja hallintainformaatiota, joka liittyy datagrammin toimitukseen. Karkeasti voisikin ajatella, että IP-osoite on suuntaa antava osoitetieto, joka määrittää, mihin lähiverkkoon datagrammi tulisi lähettää. Lähin vertailukohde reaalimaailmassa olisi Suomen postilaitoksen käyttämä postiosoite. Tällä hetkellä protokollasta on käytössä kaksi eri versiota. Ne ovat IP-versio 4, joka on toistaiseksi yleisempi, sekä pienemmässä mittakaavassa IP-versio 6, joka tarjoaa mm. laajemman osoiteavaruuden.

Transmission Control Protocol eli TCP tuottaa luotettavan bittivirtakanavan liikenteelle ja virtuaalisen kytkentäpalvelun sovelluksille. Se mahdollistaa myös pakettien uu-

delleen lähettämisen ja vuon hallinnan tiedonsiirrossa. TCP- protokolla on määritelty tarkemmin IETF RFC793 dokumentissa. (Protocols 2010, [viitattu 29.1.2010].)



*Kuvio 2. TCP ja IP- protokollien välinen suhde.*

### **2.3 Lähiverkon konsepti**

Local Area Network , joka useissa yhteyksissä lyhennetään akronyymilla LAN, tuottaa verkottumisominaisuuden joukolle päätelaitteita, jotka sijaitsevat fyysisesti toistensa lähetyvillä, kuten esim. toimistorakennuksessa, koulussa tai jopa kotona. LAN on yleishyödyllinen resurssien, kuten tiedostojen, tulostimien, pelien ja muiden sovelusten, jaossa. Useimmat lähiverkot rakentuvat verrattain halvoista materiaaleista, kuten verkkokaapelista, verkkokorteista ja kytkimistä. Mahdollisuus langattomaan siirtotiehen ja muita kehittyneitä ominaisuuksia on myös tarjolla nykyisissä lähiverkko-standardeissa.

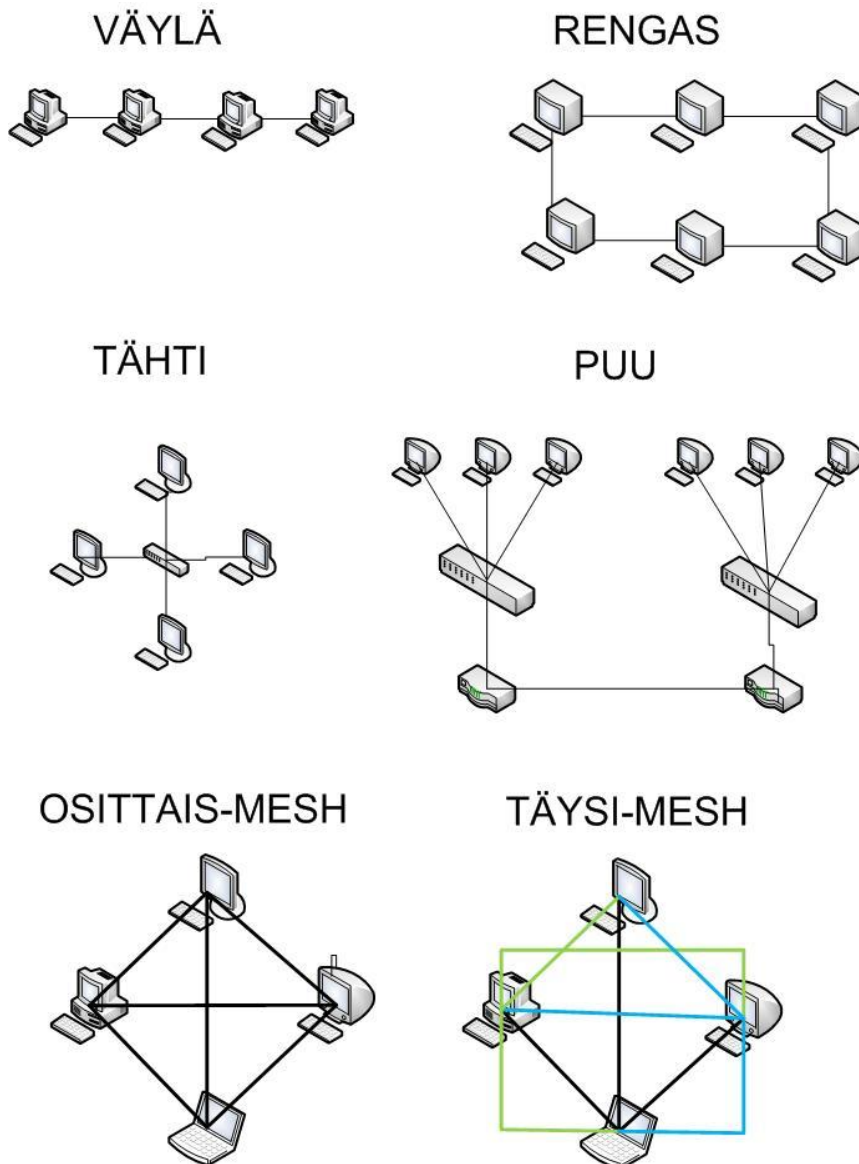
Yleisintä lähiverkkotyyppiä kutsutaan Ethernet-LANiksi (Mitchell 2010, [viitattu 28.1.2010]). Pienemmät kotiethernetit voivat koostua kahdesta päätelaitteesta, mutta suurimmat yritys- ja organisaatioethernetit koostuvat monista tuhansista päätelaitteista, jotka liittyvät toisiinsa joko verkkokaapelien ja verkkolaitteiden avulla tai langattoman siirtotien sekä tukiaseman avulla. Monet suuret ja keskisuuret LANit hajauteetaan loogisiksi ryhmiksi, joita kutsutaan aliverkoiksi.

Lähiverkon konseptiin kuuluu myös soveltuvan verkkotopologian eli verkon fyysisen mallin valinta. Vaikka topologiaa kutsutaan fyysiseksi malliksi, se ei heijasta reaali maailman asettelua, eli miten laitteet oikeasti sijaitsevat toisiinsa nähden verkossa. Esimerkiksi jos asettelet kotonasi laitteet renkaan muotoon, se ei tarkoita sitä, että siinä olisi oikeasti käytössä rengasmallin verkkotopologia.

Lähiverkkotopologiat tavallisesti jaotellaan viiteen eri kategoriaan:

- Väylä, joka käyttää yhteistä ”selkärankaa” kaikkien verkkolaitteiden yhdistämisessä lineaariseen muotoon. Yksittäinen kaapeli toimii medianana kaikille laitteille ja laitteet voivat liittyä kaapeliin vaikka t-mallisen haaroittimen avulla. Kun päätelaite haluaa kommunikoida toisen laitteen kanssa, se lähettää yleislähetysten koko väylään, mutta ainoastaan tarkoitettu kohde lukee sen.
- Renkaassa jokaisella verkkolaitteella on kaksi naapuria, joihin se on kytketty. Data liikkuu tässä topologiassa aina samaan suuntaan eli myötä- tai vastapäivään. Tämä tarkoittaa sitä, että vaurio mediassa lamaannuttaa koko verkon. Tämän vuoksi käytössä oli kaksoisrenkaat. Nykyään rengastopologia on lähes hävinnyt tapa kytkeä laitteita toisiinsa.
- Tähtimalli on tavanomaisin lähiverkkoratkaisu. Kaikki verkkoon kuuluvat laitteet yhdistyvät verkon keskipisteeseen, joka tavallisesti on kytkin omalla mediallaan. Ainoastaan verkon keskipisteen häiriöt lamaannuttavat koko lähiverkon. Muut päätelaitteet voivat tipahdella pois verkosta ja taas takaisin ilman mainittavaa häiriötä.

- Puutopologia koostuu useista yhteen liitetyistä tähdistä samassa väylässä. Verkon keskipisteen laitteet liittyvät toisiinsa median kautta puutopologian ”runggossa”. Asian voi visualisoida mielessään siten, että puun runko muodostuu keskipisteen laitteista, kuten reitittävistä kytkimistä, joista versoaa oksia eli tässä tapauksessa päätelaitteita.
- Mesh-topologia toimii tietovirran reitityksen konseptissa. Mesh-topologiassa lähetetty viesti kulkee, hieman reititysprotokollasta riippuen, joko lyhintä, nopeinta tai halvinta mediaa pitkin päästäkseen kohteeseensa. Tämä topologia on käytössä Internetin runkoverkossa (Networktutorials, 2007 [viitattu 28.1.2010]). Topologia, jossa jokainen päätelaite liittyy median kautta kaikkiin päätelaitteisiin, on nimeltään täys-mesh (full mesh). Järjestelmä, jossa jokaisella päätelaitteella on epäsuora kontakti kaikkiin laitteisiin, on nimeltään osittais-mesh (partial mesh).



Kuvio 3. Lähiverkkotopologiat.

## 2.4 Ethernet 802.3

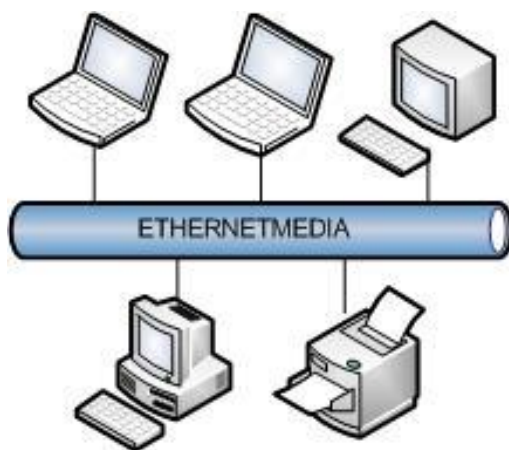
Käytetyimmät ja nopeimmat lähiverkot pohjautuvat tänä päivänä lähes kaikki pakettikytkentäiseen Ethernetiin, jonka kehitti IEEE 802.3-standardin komitea. Kuten muis-  
sakin LAN-standardeissa, se sisältää siirtotien hallintakerroksen (medium access control) sekä fyysisen kerroksen. Ensimmäisenä esitellään siis menetelmä, jota käytetään standardin mukaiseen siirtotien hallintaan, eli CSMA/CD (carrier sense multiple access/collision detection). Ytimekkäästi voisi todeta, että se kuuntelee siirtotietä ja se

sisältää metodin datapakettien törmäyksen tunnistukseen. CSMA/CD operoi neljän säännön perusteella:

- Jos siirtotie on vapaa, lähetä. Muussa tapauksessa mene vaiheeseen kaksi.
- Jos siirtotie on varattu, jatka kuuntelua niin kauan kunnes kanava on vapaa. Sitten lähetä välittömästi.
- Jos pakettien törmäys havaintaan lähetyksen yhteydessä, lähetä hetkellisesti häirintäsignaalia verkkoon. Kaikki häirintäsignaalin vastaanottaneet tahot lopettavat välittömästi lähetyksen.
- Häirintäsignaalin lähetyksen jälkeen odota satunnainen aikaväli, jota kutsutaan back off –tilaksi. Tämän jälkeen lähetä uudestaan. (Stallings 2007,488.)

Kuten CSMA-termi antaa ymmärtää, on Ethernet moniyhdysväyläinen verkko. Tämä tarkoittaa, että solmupisteet lähettävät ja vastaanottavat kehyksiä saman linkin välityksellä (Peterson 2000, 120). Karkeasti voisikin ajatella, että Ethernet on väylä, johon on kiinnitetty monia asemia, jotka kaikki kuulosteleval väylää ja heti kun väylä vaikuttaa vapaalta, niin lähetetään, jos on jotain lähetettävää kehystä.

802.3-standardi määrittelee myös laajan kokoelman eri medioita, joiden kanssa verkko voi operoida. Ne alkavat koaksiaalikaapeli-pohjaisista ratkaisuista kulkien aina 100mbit/s Fast Ethernetin kautta nykypäivän 1000 mbit/s Gigabit Ethernetiin. Näissä tapauksissa on tavallisesti käytössä kategorian 5-kierteinen parikaapeli RJ-45.



Kuvio 4. Ethernet (Pidgeon, 2010).

## Ethernetin historia

ALOHA-netiä on usein käsitelty Ethernetin henkisenä esi-isänä, koska molemmissa on protokollat lähetykselle ja lähetysvirheestä toipumiselle. Se kehitettiin 60-luvun loppupuolella Norm Abramsonin toimesta University of Hawaiissa. Toimintaperiaatteeltaan se oli digitaalinen radioverkko, joka oli suunniteltu lähettämään yksittäisiä datapaketteja saarelta toiselle. Tällainen tarvittiin siksi, että University of Hawaii oli hajajoinnettu usealle eri saarelle. Ne radioasemat, jotka halusivat asiakkuuden ALOHA-nettiin, joutuivat seuraamaan sangen yksinkertaista protokollaa:

- Jokainen asema voi lähettää paketin milloin tahansa. Pakettiin pitää merkitä digitaalisesti vastaanottajan osoite.
- Kun paketti on lähetetty, lähettävä asema jää odottamaan kuittausta (ACK) vastaanottajalta.
- Asemat kuuntelevat aina vastaanottajan osoitetta paketeista. Jos osoite täsmää kuuntelemaan asemaan, CRC-tarkistuksessa todennetaan paketin oikeellisuus. Vastaanoton onnistumisen jälkeen lähetetään lyhyt ACK-viesti.
- Jos tietyn aikavälin jälkeen ACK-viestiä ei havaita lähettävältä asemalta, oli kyseessä sitten paketin epäonnistuminen CRC-testissä tai jostakin muusta satunnaisesta syystä, tällöin paketti lähetetään uudestaan.

Lyhyesti toimintaperiaatteen voisi summata seuraavasti: ”Jos sinulla on lähetettävää, lähetä! Jos et saa kuittausta lähetä myöhemmin sama uudestaan.” Verkon teoreettinen siirtonopeus oli 9600 merkkiä/sekunnissa (Knowledge Rush 2009[viitattu 29.1.2010].)

ALOHA-netistä seuraava kehitysvaihe on enemmän Ethernetin kaltainen, Xerox-yhtymän Palo Altossa sijaitsevaan tutkimuskeskukseen pystyttämä verkko, joka oli ensimmäinen väylätopologiaan perustuva verkko. Yli kilometrin mittaiseen koaksiaalikaapeliin liitettiin yli 100 työasemaa. Tätä rakennelmaa kutsuttiin Ethernetiksi. Siinä myös ensimmäistä kertaa implementoitiin CSMA-metodi. Virhetilanteista toipuminen lisättiin metodiin 1976, jolloin CSMA-protokollaan liitettiin viite CSMA/CD. Verkon teoreettinen siirtonopeus oli 3 Mbit/s (Trendcomms 2010[viitattu 29.1.2010]).



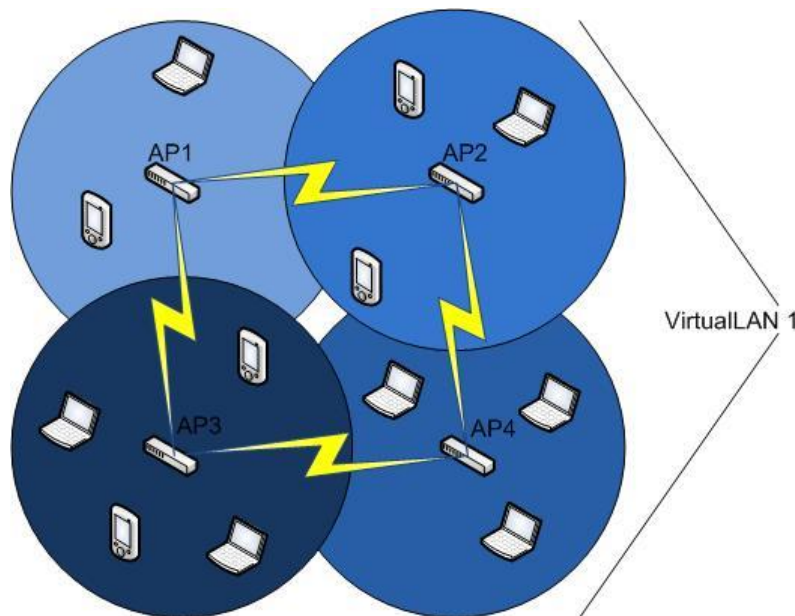
Vuoteen 1980 mennessä Xeroxin Ethernet oli niin menestynyt, että Digital Equipment Corporation, Intel ja Xerox löivät lukkoon de facto standardin 10mbit/s Ethernetiin. Tämä määritteli Ethernet II standardin, jota käytettiin pohjana IEEE 802.3 spesifikaatioon. Seuraava suurempi uudistus ajoittui vasta 90-luvun alkuun, jolloin siirryttiin koaksiaalikaapelista kierteiseen parikaapeliin, mutta toki vuosikymmenessä Ethernetin siirtonopeudet myös kasvoivat merkittävästi. Vuonna 1995 standardi 100 mbit/s Ethernetiin julkaistiin ja sitä kutsuttiin Fast Ethernetiksi. Tätä kirjoittaessa 100 gbit/s Ethernetin mahdollistava teknologia on prototyypivaiheessa ja sen lopullinen implementaatio laitekantaan on vielä epävarmaa.

## **2.5 Langaton siirtotie lähiverkossa**

Langaton lähiverkko eli WLAN käyttää hajontaspektriä lähetyksessä 902 Mhz:n taajuutta 802.11 -standardissa, sekä 2.4 Ghz:n taajuutta 802.11-standardin laajennuksissa b ja g. Hajontaspektrin yhdistäminen lähetyksen luonteeseen matalalla virransyötöllä, 30-100 mW:n alueella, tarkoittaa sitä, että yksittäinen verkon käyttäjä ei häiritse toista käyttäjää, koska hajontaspektri lähetyksissä levittää radiosignaalin yli laajan taajuusalueen. (Wilson 2008, 244.) Standardiperheessä 802.11 on käytössä myös CSMA/CA (Collision Avoidance) eli pääpiirteiltään Ethernetistä tuttu siirtotien varaus, mutta tällä kertaa törmäystä ei tunnisteta vaan vältellään. Käytännössä se tapahtuu laittamalla lähetyksen pituus siksi aikaa, kunnes siirtotie, eli tässä tapauksessa tietty aallonpituus, vapautuu muista signaaleista. Muut tukiasemat tietävät tuloillaan olevan lähetyksen siitä, että lähetystä valmisteleva tukiasema lähettää siirtotietä varaavan signaalin hetkeä ennen varsinaista lähetystä (ATIS 2007, [viitattu 29.1.2010].) Modernit langattomat lähiverkot pohjautuvat lähinnä 802.11b-standardiin.

Puhuttaessa langattomasta lähiverkosta vastaan tulee lähes välittömästi termi Wi-Fi. Se on The Wireless Ethernet Compatibility Alliancen sertifiointiohjelma. Ohjelmassa tarkoituksena on varmistaa, että kaikki IEEE 802.11-päätelaitteet ovat käytännössä oikeasti yhteensopivia. Verrattain sama tilanne on IEEE 1394 -standardin liitännän kanssa. Tämä liitäntä tunnetaan paremmin nimellä Firewire.

Keskeinen etu langattomassa lähiverkossa on sen tuottama fyysinen vapaus RJ-45 verkkokaapelista ja liitännästä seinäpistokkeeseen. Kuten lukija voi helposti kuvitella, on tämä selkeä etu esimerkiksi modernissa toimistoympäristössä, jossa verkkoon on liitetty mm. kannettavia multimediapäätteitä, matkapuhelimia sekä kannettavia tietokoneita. Tukiasemien pienitehoiset antennit pystyvät helposti tuottamaan kentän, joka kantaa hyvin usean kuivalevyseinän lävitse. WLAN- teknologian ansiosta ei ole tarpeen uusia koko osaston fyysistä kaapelointia, kun uusia päätelaitteita asennetaan. Suuria kustannussäästöjä syntyy myös, kun verkkoa laajennetaan. Tällöin jokainen uusi toimisto tai konferenssihuone ei tarvitse omaa fyysistä liitosta runkoverkkoon, vaan usein riittää, että ainoastaan tukiasemilla on fyysinen yhteys kytkimiin. Tämä säästää sekä aikaa että rahaa.



*Kuvio 5. Monta tukiasemaa samassa virtuaali-LAN:ssa.*

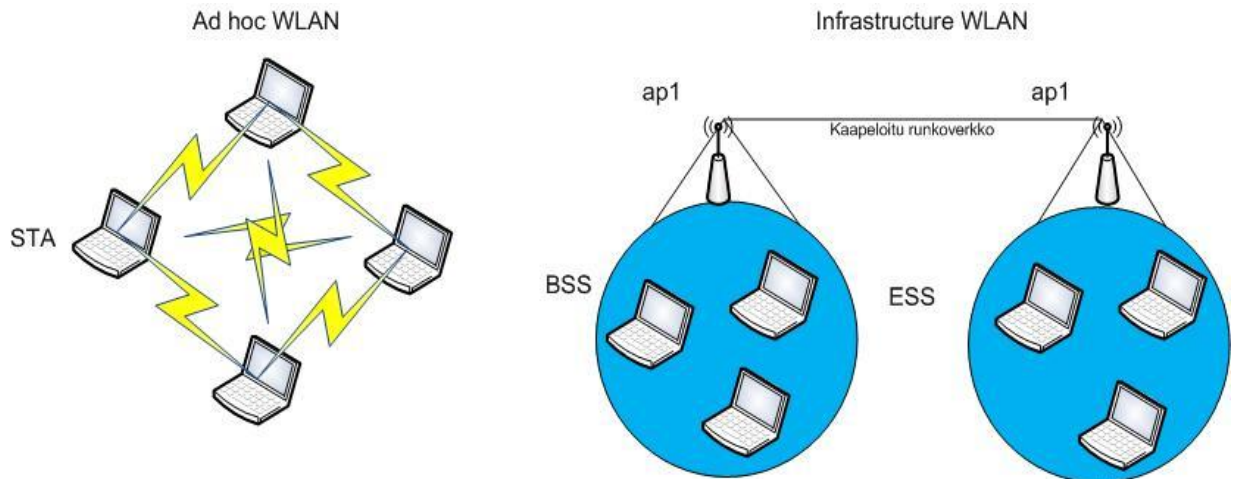
Yleensä tarvitaan useita tukiasemia, jotta verkon kokonaispeitto olisi mielekäs esimerkiksi oppilaitoskäytössä. Tällöin useita tukiasemia voidaan liittää yhteen samaan virtuaalisen lähiverkkoon, jolloin peittoalueella operoitu päätelaite toimii samoilla asetuksilla joka puolella peittoaluetta.

## **Arkkitehtuurit**

Basic service set on IEEE 802.11-standardin perusmoduuli. Infrastruktuurimoodissa yksittäistä access pointia (AP) ja siihen liittyviä asemia (STA, associated stations) kutsutaan BSS:ksi. Tätä ei kuitenkaan tule sekoittaa yksittäisen AP:n kuuluvuusalueeseen, jota kutsutaan basic service set areaksi (BSA). Järjestelmä, jossa kaikki STA:t liittyvät yhteen master AP:hen, kutsutaan infrastruktuurimoodiksi. Tässä järjestelmässä verkon nimeä eli SSID:tä lähettää tukiasema. Järjestelmää, jossa kaikki kantoalueella olevat STA:t muodostavat keskenään yhteen liitetyn verkon, kutsutaan Ad-hoc-verkoksi. Ad-hoc-verkon nimeä lähettää satunnaisessa järjestyksessä jokainen verkkoon liittynyt STA.

Oleellista on vielä esitellä extended service set, eli monen BSS:n yhteenliittymä, jossa kaksi tai useampia LANeja yhdistyy. Tämä kokonaisuus esiintyy yksittäisenä BSS:nä LLC-kerroksella jokaiselle laitteelle, joka liittyy BSS:ään. LLC-kerros on siirtokerroksen toinen tärkeä komponentti toisen ollessa MAC-kerros (Stallings 2007,75). Yhteen liittyneiden BSS:ien joukolla pitää olla sama verkon nimi eli SSID. Tukiasemat voidaan määrittää toimimaan kaikki samalla kanavalla tai ne voidaan lomittaa toimimaan kaikki eri kanavilla läpimenon jouduttamiseksi.

Voisi ajatella, että infrastruktuurimoodi seuraa tähtitopologiaa ja Ad-hoc-arkkitehtuuri kiertosuunnatonta rengasta. Usein Ad-hoc-verkkoa verrataan myös vertaisverkkoon, jossa jokainen verkkoon liitetty päätelaite on tasa-arvoinen verkon jäsen. Hyödyllisiä käyttökohteita Ad-hoc-verkolle on verkkoresurssien, kuten tiedostojen tai verkkotulostimen, jako välittömässä lähipiirissä. Infrastruktuuriarkkitehtuurin käyttökohteet ovat sitten enemmän samankaltaiset kuin tavallisen kaapeloidunkin lähiverkon eli usean päätelaitteen portti verkkoon.



Kuvio 6. Ad-hoc ja infrastruktuuri- verkkojen väliset erot (Stallings 2007, 527).

## 2.6 WLANin sijoittuminen OSI-malliin

Seuraavaksi tarkastellaan pelkän 802.11-standardin määrittelemää langatonta lähiverkkoa teoreettisella tasolla. Tällöin WLAN on pelkästään fyysisen kerroksen kantoaallon modulaatiota, siirtotien käyttöä ennalta määritetyillä aallonpituuksilla ja lähetysten vastaanottoa. Siirtyessä käytännön sovelluksiin otetaan käyttöön koko OSI-malli. Kuviossa 7 jo tuttua OSI-mallia laajennetaan ottamalla käytäntö mukaan siten, että jokaiselle kerrokselle on lisätty verkkolaite, joka operoi kyseisellä kerroksella.

Käytännön hyötyä OSI-mallista on visuaalisena työkaluna verkon vikatilanteiden selvityksessä. Tästä esimerkkinä voisi olla tilanne, jossa saadaan puhelu asiakkaalta, joka väittää, ettei pysty avaamaan yhtäkään Internet-sivua. Vikatilanteiden haarukointiin on pääsääntöisesti kaksi eri metodia, jotka ovat top to bottom (hajottava) ja bottom up (koostava). Esimerkkitapauksessa olisi järkevintä aloittaa bottom up –metodilla. Järkevä vian haarukointi kulkisi siis näin:

- Onko verkkokaapeli kytketty oikein? (fyysinen)
- Palaako/vilkkuuko valo kytkimessä? Entä verkkokortissa? (siirto)
- Saatko IP-osoitteen? (verkko)
- Pystytkö pingaamaan verkon oletusyhdyskäytävää? (verkko, testaa samalla lähiverkon toiminnallisuuden)

- Saatto DNS-palvelimen tiedot? (verkko)
- Pystytkö pingaamaan DNS-palvelinta? (verkko, testaa lähiverkon liitoksen WANIin)
- Miten palomuurisi asetukset ovat? (verkkokerrokselta ylöspäin aina sovelluskerrokselle asti)
- Pystytkö pingaamaan nimeä verkossa, esimerkiksi [www.google.com](http://www.google.com) osoitetta? (sovellus, DNS ja verkon yhteys WANIin)
- Pystyykö verkkoselaimesi avaamaan jotain toista, täysin satunnaista sivustoa? (kaikki kerrokset)

Jos vastauksena on kaikkiin kohtiin kyllä, niin vika ei ole paikallisessa lähiverkossa, päätelaitteessa tai käyttäjässä.

| KERROS  | TOIMINTO   | PROTOKOLLAT   | VERKKOKOMPONENTTI  |
|---|--|---|--|
| Sovellus<br><ul style="list-style-type: none"> <li>Käyttöliittymä</li> </ul>                  | <ul style="list-style-type: none"> <li>Käyttäjän liittyminen verkkoon</li> </ul>   | <ul style="list-style-type: none"> <li>DNS, FTP</li> <li>SMB</li> <li>SMTP</li> </ul>   | <ul style="list-style-type: none"> <li>Gateway</li> </ul>  |
| Esitystapa<br><ul style="list-style-type: none"> <li>Kääntäjä</li> </ul>                      | <ul style="list-style-type: none"> <li>Kääntää sovellukselta verkkoon sopivaan formaattiin ja päinvastoin</li> <li>Muuntaa kaikki formaatit kaikista lähteistä yhteiseen muotoon</li> </ul>  | Ei tarvitse aina implementoida verkkoprotokollaan   | <ul style="list-style-type: none"> <li>Gateway</li> <li>Redirector</li> </ul>  |
| ISTUNTO<br><ul style="list-style-type: none"> <li>Synkronisaatiota ja istuntoja</li> </ul>    | <ul style="list-style-type: none"> <li>Aloittaa, ylläpitää ja lopettaa istuntoja</li> <li>Halinnoi kuka voi lähettää ja kuinka pitkään</li> <li>Tunnistaminen nimen perusteella</li> </ul>   | <ul style="list-style-type: none"> <li>NetBIOS</li> <li>Mail Slots</li> <li>RPC</li> </ul>  | <ul style="list-style-type: none"> <li>Gateway</li> </ul>  |
| KULJETUS<br><ul style="list-style-type: none"> <li>Paketit ja virheistä toipuminen</li> </ul> | <ul style="list-style-type: none"> <li>Vuon hallinta</li> <li>Virheiden käsittely</li> <li>Uudelleenlähetyt virhetilanteissa</li> </ul>  | <ul style="list-style-type: none"> <li>TCP</li> <li>ATP</li> <li>NetBIOS</li> </ul>   | <ul style="list-style-type: none"> <li>Gateway</li> <li>B-reititin</li> </ul>  |
| VERKKO<br><ul style="list-style-type: none"> <li>Osoitteet ja reititys</li> </ul>             | <ul style="list-style-type: none"> <li>Muuntaa loogiset verkko-osoitteet fyysisiksi osoitteiksi</li> <li>Pilkkoo protokollaan sopimattoman suuret kehykset pienemmiksi yksiköiksi</li> </ul> | <ul style="list-style-type: none"> <li>IP</li> <li>ICMP</li> <li>DECnet</li> <li>RIP</li> <li>OSPF</li> </ul>   | <ul style="list-style-type: none"> <li>Reititin</li> <li>ATM-kytkin</li> </ul>   |
| SIIRTO<br><ul style="list-style-type: none"> <li>KEHYKSISTÄ BITTEJÄ</li> </ul>                | <ul style="list-style-type: none"> <li>Vastuussa kehyksien virheettömästä kuljetuksesta fyysistä kerrosta käyttäen</li> </ul>  | <ul style="list-style-type: none"> <li>Logical link control(LLC)</li> <li>Virheiden valvonta</li> <li>Tietovuon hallinta</li> </ul> <hr/> 802.1 OSI-malli<br>802.2 LLC<br><hr/> <ul style="list-style-type: none"> <li>Media Access Control(MAC)</li> </ul> Kommunikoi liitäntäkorttine kanssa<br><hr/> 802.3 CSMA/CD (Ethernet)<br>802.4 Token bus<br>802.5 Token ring | <ul style="list-style-type: none"> <li>Siltain</li> <li>Kytkin</li> <li>ISDN reititin</li> <li>Verkkokortti</li> </ul> |
| FYYSINEN<br><ul style="list-style-type: none"> <li>BITTIVIRTAA MEDIASSA</li> </ul>            | <ul style="list-style-type: none"> <li>Määrittää kaapelit, verkkokortit</li> <li>Liitoskohta verkkokorttiin</li> <li>Tekniikan, jolla bittivirtaa liikutellaan</li> </ul>                    | <ul style="list-style-type: none"> <li>IEEE 802</li> <li>IEEE 802.2</li> <li>ISO 2110</li> <li>ISDN</li> </ul>  | <ul style="list-style-type: none"> <li>Toistin</li> <li>Hub</li> <li>Oskiloskooppi</li> <li>Vahvistin</li> </ul>       |

Kuvio 7 OSI-malli (Petri 2009,[viitattu 25.2.2010]).

## 2.7 IEEE 802.11

Institute for Electrical and Electronics Engineers (IEEE) on teollisuusyhteenliittymä, joka on monia vuosia kehittänyt teollisia standardeja. Nämä standardit vaikuttavat suuresti sähkölaitteisiin, joita käytetään kotona sekä työpaikoilla. Tällä hetkellä IEEE 802.11b+g- standardipari on ylivoimainen markkinajohtaja langattomissa lähiverkoissa, jos lasketaan markkinaosuuksia sekä kentällä olevia aktiivisia tukiasemia. Tuotteet, jotka olivat yhteensopivia 802.11b+g- standardin kanssa, eivät suinkaan olleet ensimmäisenä markkinoilla. Nykyisin se on kuitenkin dominoivin esiasennettu pohja. Syy tähän selventyy syventymällä hetkeksi kuvioon 8.

Nykyään uusi 802.11n-laajennus, joka on esi-standardi vaikka markkinoilta löytyy kattavasti n-standardin verkkolaitteita, on valtaamassa markkinaosuutta kasvavalla vauhdilla b+g standardilta ja on arvioitu, että vuoteen 2012 mennessä se olisi käytetyin standardi. 802.11n-standardissa on riittävä kaistanleveys esim. HD-tason elokuvan streamaukseen verkon yli. Ainoana kompastuskivenä standardin kanssa vaikuttaa olevan sen tarvitsema kohonnut virransaantivaatimus (Wi Revolution 2008,[viitattu 3.2.2010]). Tämä on ongelmallista esimerkiksi matkapuhelimissa, joissa on sisäinen WLAN-moduuli.

| Langaton Standardi   | 802.11b   | 802.11a  | 802.11g   |
|----------------------|---|--|---|
| Yleisyys             | Laajasti käytetty   | Edelleen "uutta tekniikkaa" Jää n-standardin jalkoihin                           | Uutta tekniikkaa Suurin kasvu   |
| Nopeus, teoreettinen | 11Mbp/s   | 54Mbp/s  | 54Mbp/s   |
| Taajuus              | Häiriöinen 2.4GHz. Paljon lähettäviä asemia aallonpituudella. Lisäksi mm. mikroaaltouunit ylikuuluvat | Suhteellisen vapaa 5GHz. Toimii rinnan 2.4GHz asemien kanssa ilman ylikuulumista | Häiriöinen 2.4GHz. Paljon lähettäviä asemia aallonpituudella. Lisäksi mm. mikroaaltouunit ylikuuluvat |
| Kantomatka           | Sisätiloissa 100-150metriä. Riippuen paljon rakennusmateriaaleista                                    | 25-75metriä. Ottaa vähemmän häiriötä, johtuen vapaasta aallonpituudesta          | Sisätiloissa 100-150metriä. Riippuen paljon rakennusmateriaaleista                                    |
| Julkiset AP          | Lähes kaikki julkiset "hotspotit" tukevat   | Ei ole. Johtuen pääsääntöisesti kurjasta kantomatkasta ja kaistanleveydestä      | Lähes kaikki julkiset "hotspotit" tukevat   |
| Yhteensopivuus       | Yleisesti käytetyin   | Ei ole yhteensopiva B ja G laajennuksien kanssa                                  | Toimii rinnan 802.11b kanssa (11Mbp/s nopeudella). Ei 802.11a kanssa                                  |

Kuvio 8. WLAN-standardit.)

## **3 KÄYTÄNNÖN SOVELLUKSET**

### **3.1 Wi-Fi**

Vuonna 1999 useat johtavat langattomia verkkolaitteita valmistavat tahot muodostivat voittoa tavoittelemattoman Wireless Ethernet Compatibility Alliance (WECA)-organisaation. Tämä ryhmä sittemmin nimesi itsensä uudelleen Wi-Fiksi, joka käynnisti Wi-Fi-certified sertifiointiohjelman vuonna 2000. Se koostuu tänä päivänä yli 200 jäsenyrityksestä, jotka valmistavat tai ylläpitävät langattomia verkkolaitteita. Alianssin pääsääntöinen funktio on varmistaa, että IEEE 802.11-standardin tuotteet eri valmistajilta todella toimivat yhdessä.

Wi-Fi-allianssi on mm. tuottanut testauspaketin, joka määrittelee, miten jäsenyritysten laitteita tulisi testata itsenäisissä testilaboratorioissa. Tuotteet, jotka läpäisevät testit, saavat oikeuden Wi-Fi-tuotemerkkiin, joka on yhteensopivuuden merkki. Paikallistamalla Wi-Fi-sertifikaatin laitteen myyntipakkauksesta kuluttaja voi olla lähes 100-prosenttisen varma, että hankinnassa oleva laite toimii jo olemassa olevien Wi-Fi-sertifikaatin laitteiden kanssa. Lisäksi nykyiset spesifikaatiot määrittävät, että uusien laitteiden pitää olla myös alaspäin yhteensopivia vanhempien laitekantojen kanssa a-standardia lukuun ottamatta (Wi-Fi Alliance 2009, [viitattu 3.2.2010]).

Wi-Fi-tuotemerkkiä tutkiessa tulee sangen usein vastaan toinen vastaavanlainen akronyymi eli WiMAXiin. Näiden kahden sertifikaatin erot ovat lähinnä implementaatiokohteen kokoluokassa. Wi-Fi on tarkoitettu pienemmän mittakaavan LANeihin, kun taas WiMAX määrittelee spesifikaation MAN-tason verkoille (metropolitan area network).

### **3.2 Standardit a-n**

Kuten aikaisemmin tässä työssä on todettu, käytännön sovellukset 802.11-standardista jakautuvat neljään eri kategoriaan. Näistä a-kategoria on käytännössä hävinnyt arkisesta käytöstä ja n-standardi odottaa vielä lopullista läpilyöntiään. Se tapahtunee vuoteen 2012 mennessä.



N-kategoria ratifioitiin lokakuussa 2009. N-standardi laajentaa Wi-Fi tuoteperhettä mm. moniantennituella (MiMo). Muita tässä samassa yhteydessä mainittavia mielenkiintoisia kehityskohteita on 802.11y, joka tulee toimimaan 3650-3700 Mhz:n kaistalla. Tämä samainen kaista oli alun perin käytössä Yhdysvalloissa analogisissa tv-lähetyksissä, mutta se jää vapaaksi, kun maan tv-lähetykset digitalisoidaan. Se, mikä tekee mainitusta taajuusalueesta mielenkiintoisen, on sen pitkät aallonpituudet, joiden ominaisuuksiin kuuluu mm. vahva rakenteiden läpäisy ja kantomatka tukiasemasta. Mahdollisuus olisi siis rakentaa @450-tyyppinen järjestelmä käyttäen osittain vanhaa tv-lähetystekniikkaa.

Numeraaliset erot eri kategorioiden välillä voi tarkistaa kuviosta 8. Loput keskeiset viisi eroavaisuutta ovat:

*Nopeus:* 802.11a- ja g-verkot ovat lähes viisi kertaa nopeampia kuin alkuperäinen b-verkko. N-verkko on taas lähes viisi kertaa nopeampi kuin tämän hetkiset g-järjestelmät (Briere, Hurley & Ferris 2008, 22). Yleensä verkkoliikenteen pullonkaula ei ole 54mbit/s nopeus, joka on b+g standardin teoreettinen maksimi, vaan asiakaslinjan kaista. N-standardin tuoma laajennus nopeuteen tulee olennaiseksi vasta, kun lähiverkossa siirretään HD-tason videokuvaa.

*Hinta:* 802.11g-verkkolaitteet, jotka ovat tämän päivän de facto- standardi, ovat olleet nykyhetkessä markkinoilla kohta neljä vuotta. Tästä johtuen niiden hinnat ovat varsin alhaiset. Tämän lisäksi useimmissa kolmen vuoden sisällä ostetuissa kannettavissa päätelaitteissa on sisäänrakennettu tuki sekä b- että g-standardeille.

*Radiosignaalin kantama:* 802.11a-järjestelmissä on pääsääntöisesti lyhyempi kantomatka kuin saman tehoisilla b- ja g-järjestelmillä. Käytännön kantomatka on sitten paljon enemmän riippuvainen rakenteista.

*Häiriöt siirtotiessä:* 2.4 GHz:n taajuuteen aiheuttavat monet jokapäiväiset laitteet häiriöitä ja yleisesti ottaen se on myös kovin ruuhkainen. Häiriöitä aiheuttavat pääsääntöisesti mikroaaltouunit, matkapuhelimet ja muut päätelaitteet, jotka käyttävät samaa

kanavaa. A-standardin käyttämä viiden Ghz:n alue on paljon vapaampi satunnaisesta kohinasta ja muista päätelaitteista.

*Yhteensopivuus:* Koska 802.11a ja 802.11b/g käyttävät eri aallonpituuksia ja eri kantoaallon modulaatioita, ne ovat täysin yhteensopimattomia alkaen rautatasolta. On tosin olemassa varsin kalliita verkon tukiasemia, jotka tukevat kaikkia kolmea standardia. Lisäksi päätelaite, joka tukee ainoastaan 802.11a-standardia, on varsin harvinaisen.

Mainio vertauskuva nykyisiin b/g-standardin laitteisiin on vanhat AM/FM-radiot. AM- ja FM- signaalin vastaanotossa on varsin radikaalit eroavaisuudet, mutta tuskin kukaan osti aikoinaan radiolaitetta, joka kykeni ottamaan vastaan vain AM- tai FM-signaalia. Käyttäjä sai tarpeen mukaan valita kumpaa signaalia vastaanottaa. Samoin on nykyisissä WLAN-päätelaitteissa, joissa loppukäyttäjä saa itse päättää kummassa operoidaan, b- vai g-standardissa. Nykyisin on myös mahdollista asettaa laite toimimaan b+g- tilassa, jossa päätelaite ja AP keskenään sopivat, kumpaa standardia käytetään.

### **Horisontissa UWB**

Ultra Wideband Radio lähettää digitaalisia pulsseja eli impulsseja, jotka eroavat radioaaltojen sini-aallosta huomattavasti.. Laitteet lähettävät samanaikaisesti signaalia yli hyvin laajan spektrin. Lähetin ja vastaanotin toimivat yhteistyössä nanosekunnin tarkkuudella tietäen, milloin lähettää ja milloin vastaanottaa pulssia. UWB tarjoaa siirtotien hyvin nopeaan tiedonsiirtoon, mutta se tekee sen myös häiriöttömästi ja ilman ns. monen siirtotien häiriötä.

Monen siirtotien häiriö -ilmiö tapahtuu, kun sama kehys saapuu vastaanottajalle monia eri polkua pitkin signaalin kimpoamisen takia. Signaaliin lähtee lähettäjältä epäsuunnattuna säteilyä ja se ottaa varsin hyvin kimmoketta esim. peileistä. Tätä häiriötä ei tapahdu UWB- menetelmässä, koska se sisältää varsin tarkan ikkunan eli time gaten, joka kuvaa vastaanottajalle nanosekunnin tarkkuudella ikkunan, jolloin sen olisi

syötä vastaanottaa seuraavia kehyksiä. Täten lähettäjä pystyy hylkäämään kehykset, jotka saapuvat multipath- ilmiön takia uudestaan. IEEE-työryhmä on antanut protokollalle nimen 802.15.3a

Haittapuolena teknologiassa on jo teoriatasolla sen verrattain heikko kantama, joka jää alle 20 metriin. Toisaalta tämän 20 metrin sisäpuolella se teoriassa kykenisi jopa 110 mbit/s nopeuksiin ja lähempänä eli neljän metrin sisällä noin 480 mbit/s nopeuteen (Prossori 2004, [viitattu 4.2.2010]).

UWB tulisi korvaamaan sangen yleisesti esimerkiksi matkapuhelimien välisessä tiedonsiirrossa käytetyn Bluetooth –toiminnallisuuden. Teoreettinen kapasiteetti riittäisi kuitenkin mainiosti esimerkiksi langattoman Ad-hoc- tyyppisen lähiverkon rakentamiseen, jossa verkkoon kuuluvat laitteet toimisivat toistensa relay-asemina välittäen kehyksiä aina MAN-linkkiin asti.

### **3.3 Langattoman verkon keskeiset laitteet**

Yksinkertaisimmillaan langaton verkko tarvitsee ainoastaan tukiaseman ja päätelaitteen, mutta tukiasema itsessään olisi täysin hyödytön, jos sillä ei olisi reittiä ulos MAN-verkkoon. Täten tarvittavien laitteiden listaan pitää lisätä vielä reititin, joka hallitsee yhteyden muodostamisen ulos. Kotiolosuhteissa yleensä nämä kaksi laitetta on yhdistetty yhdeksi kokonaisuudeksi, ja tällöin laitetta kutsutaan integrated system routeriksi. Tämän lisäksi tarvitaan kaksi antennimoduulia, toinen päätelaitteelle ja toinen tukiasemalle, jotta signaalin lähetys ja vastaanotto sujuu optimaalisemmin. Tukiasema on tavanomaisesti kytköksissä reitittimeen kategorian viisi tai kuusi kierretyllä parikaapelilla, joten se otetaan myös laskuihin keskeisenä komponenttina.

Pullonkaulana sisäverkossa on b/g- standardia käyttäen langattoman siirtotien 54mbit/s siirtonopeus ja ulkoverkkoon suuntautuvassa liikenteessä pääsääntöisesti oman tilaajakaistan leveys. Kategorian 5e, joka on yleisin lähiverkkokaapelointiin käytetty verkkokaapeli, teoreettinen maksimi siirtonopeus on noin 550mbit/s, joten se ei ole missään SOHO (small office and home)-ratkaisussa pullonkaula. Suuremmissa

lähiverkkoratkaisuissa alue- ja nousukaapelointia varten saattaa nousta tarve siirtyä optisen kuitukaapelin käyttöön, mutta tällöin verkkoa kuormittavia laitteita on pääsääntöisesti satoja, mahdollisesti myös palvelimia.

Antennimoduulin fyysinen ulkoasu saattaa vaihdella valmistajalta toiseen, mutta kaikki ovat kuitenkin ympärisäteileviä eli omnidirektionaalisia radiomastoja. Voisi kuvitella, että antennimoduuli projisoi ympärilleen näkymättömän pallon, jonka summitaisessa keskipisteessä antenni sijaitsee. Uusin 802.11n-standardi sisältää kehittyneemmän signaalin prosessoinnin ja mahdollisuuden tehokkaaseen MiMo-järjestelmään. 802.11n:ssä on myös mahdollisuus muovata kenttää, jota antenniryppäs lähettää (Briere et al. 2008, 40).

Tavallisesti kannettavissa tietokoneissa WLAN-piirisarja on eriytetty muista komponenteista erilliselle piirilevylle, koska radiokomponenttina se saattaa aiheuttaa häiriöitä mm. prosessorin ajoituskellopulsseille. Tästä piirisarjasta lähtee yhdestä kolmeen antennikaapelia, jotka kiertävät rakenteiden läpi päätyen lopulta metallilaattaan, joka tavanomaisesti kiinnitetään laitteen näyttömoduulin yläreunaan parhaan kuuluvuuden saamiseksi. Matkapuhelimissa WLAN-antennimoduuli on integroitu tavanomaisen RF-antennin rinnalle. Poikkeuksia totta kai on, mutta tavanomaisesti WLAN-piirisarja on eriytetty muista komponenteista, antennissa on pinta-alaa ja se on sijoitettu mahdollisimman kauas lämmön lähteistä, koska konduktanssiin vaikuttaa johtimen lämpötila. Jos mahdollista, laitteessa olisi myös hyvä olla aux-antenni mainantennin lisäksi.

Reititin on laite, joka yleisellä tasolla yhdistää kaksi lähiverkkoa toisiinsa mahdollisimman lyhyttä, nopeinta tai halvinta reittiä käyttäen. Reititin toimii IP-osoitteiden tuottaman informaation ja valitun reititysprotokollan avulla. Tavanomaisimpia reititysprotokollia ovat RIP v2 ja OSPF. Karkeasti voisi kuvitella, että reititin hoitaa liikenteen kytkimelle asti, joka sitten toimittaa paketin oikealle vastaanottajalle käyttäen MAC-osoitetietoja. Ajatusleikkinä reititystietoa voi verrata postinumeroon ja lähiosoitetta MAC-osoitteeseen. Kuten aiemmin todettiin, tavanomaiset kotona ja pien-toimistoissa käytettävät WLAN-tukiasemat sisältävät myös reititintoiminallisuuden.

### 3.4 Tukiaseman kuuluvuus

Seuraavassa lyhyt katsaus keskeisiin seikkoihin, jotka vaikuttavat tukiaseman kuuluvuuteen jos se sijoitetaan sisätiloihin.. Listassa ei tietenkään luetella aivan kaikkia ilmiöitä, jotka saattavat huonontaa lähetystehoa tai vastaanottoa, kuten auringon aktiiviset hetket tai häiriöt sähköjen jakeluverkossa.

*Tukiaseman lähetysteho.* Tämä tarkoittaa tukiaseman tehoa radiolähettimeen. Yleensä asetuksissa, jos laite sitä tukee, on mahdollista säätää tätä erikseen kohdassa transmission power tai TX power. Loogisesti, mitä enemmän tehoa radiopiiri saa, sen pidempi on sen kantomatkka. Wi-Fi sertifioitujen tukiaseman lähetystehon tulee olla alle 30dBm eli yksi watti (Briere et al. 2008, 40). Tämän lisäksi telehallintaviranomainen on määrittänyt maksimitehon, jolla sisätiloissa sijaitsevaa tukiasemaa saa käyttää. Se on 13dBm:n ja 15dBm:n välissä. Kuten aikaisemmin todettiin, mitä enemmän tehoa, sitä voimakkaampi signaali ja laajempi kantoalue. Radiotekniikassa dBm tarkoittaa desibelimäärää suhteessa milliwattiin. Tätä yksikköä käytetään erityisesti radiotekniikassa.

*Antenna gain.* Tukiaseman antenni tai antennijärjestelmät tuottavat paremman saannin eli gainin tukiasemaan. Tietyissä malleissa on mahdollisuus vaihtaa herkempään antenniin, ja se tuottaa lisäsuorituskykyä, mitä ei saada enää esimerkiksi lisäämällä lähetystehoa. Vertailukohta gainiin löytyy musiikin maailmasta. Yksinkertaistetusti gain määrittää paljonko volyymia on käytössä, eli piirisarjan kykyä lisätä tehoa. Käytössä on myös termi antennin hyötysuhde suomenkielisessä kirjallisuudessa.

*Antennin tyyppi.* Radioantennit sekä lähettävät että vastaanottavat signaalia. Erimalliset antennit lähettävät signaalia erilaisissa kuvioissa. Tyypillisin antennimalli on dipoliantenni, joka lähettää signaalia, kuten aiemmin on todettu, tasaisesti joka suuntaan. Käytännössä kentän muoto on donitsimainen puikonmallisen antennin vuoksi. Tämä tarkoittaa sitä, että alueet suoraan tukiaseman alla tai yläpuolella ovat heikosti kuuluvia. Esimerkiksi Buffalon valmistamiin tukiasemiin on saatavilla antenneja, jotka mahdollistavat suunnatut lähetykset. Radioaaltoja ei voi kuitenkaan efektiivisesti täy-

sin suunnata siten, että ne kuuluisivat vain ja ainoastaan tietyllä alueella, koska ne kimpoilevat materiaaleista ja antennin tyypistä riippumatta signaali aina säteilee hie-  
man omnidirektionaalisesti. Kohteissa, joissa ilmenee tarvetta rajoittaa tarkasti WLAN-kenttä tiettyyn kiinteistöön, olisi syytä turvautua radioaaltoja vaimentaviin seinä- ja ikkunamateriaaleihin sen sijaan, että yritettäisiin rajoittaa signaalin lähetystä.

*Signaalin attenuaatio* Joissakin lähteissä tätä kutsutaan leikkisästi signaalin sukupuutoksi, joka itse asiassa kuvaa tilannetta varsin mainiosti. Se aiheutuu esteistä ja väli-  
matkasta matkalla lähettävältä taholta takaisin tukiasemalle. Hyvä vertauskuva tilan-  
teeseen on kirkas talvipäivä, signaali on auringon valo ja vastaanottava taho silmät. Otetaan käyttöön aurinkolasit, jotka tuottavat huomattavaa attenuaatiota jo näkyvällä spektrillä. Luvussa 3.4 käsitellään tarkemmin tavanomaisimpia attenuaatioiden eli häi-  
riöiden tuottajaa.

### 3.5 Siirtotien häiriöiden lähteet

Kuten on monta kertaa aikaisemmissa luvuissa todettu, on 2.4 Ghz:n kaista varsin ruuhkainen. Tämä johtuu mm. 802.11b+g:n yleisyydestä ja muista radioteknisistä häi-  
riölähteistä kuten matkapuhelimista, mikroaaltouuneista sekä nykyisin myös langat-  
tomista osoitinlaitteista, jotka kaikki käyttävät hyväkseen 2.4 Ghz:n kaistaa. Ongel-  
maa korostaa vielä se seikka, että useimmat tukiasemat automaattiasetuksilla jäävät  
käyttämään keskialueen kanavia, joten tavanomaisesti käytetään ruuhkautuneen kais-  
tan ruuhkautuneita kanavia. Kuviossa 9 on lueteltuna yleisimmät attenuaation lähteet  
alkaen pahimmista ja päättyen lähes olemattomiin esteisiin.

| Este              | Attenuaation määrä | Esimerkki                          |
|-------------------|--------------------|------------------------------------|
| Peilipinnoite     | Hyvin suuri        | Peili                              |
| Teräs             | Hyvin suuri        | Vahvike mat. turvaovet ym.         |
| Betoni            | Suuri              | Lattia, ulkoseinä, tukipilarit     |
| Paperi            | Suuri              | A4riisi, paperipaali               |
| Keraamiset laatat | Suuri              | Keraamiset levyt, lattiamateriaali |
| Marmori           | Keskitaso          | Julkisivut, lattia                 |
| Tiili             | Keskitaso          | Julkisivut, lattia                 |
| Vesi              | Keskitaso          | Akvaario, kostea puu julkisivussa  |
| Lasi              | Matala             | Ikkunat ym                         |
| Synteettiset mat  | Matala             | Eriöt                              |
| Laasti            | Matala             | Julkisivut                         |
| Puu               | Matala             | Julkisivut                         |

Kuvio 9. Attenuaation lähteet (Briere 2008,104).

Kuviosta 9 voi poimia helposti sen, että teräsvahvisteiset betonirakenteet väliseinärakennelintana ovat varsin huono kokonaisratkaisu, jos rakennusta lähtökohtaisesti suunnitellaan käytettäväksi esimerkiksi toimistotilana, johon olisi myöhemmin tarkoitus asentaa langattomasti toimiva lähiverkko. On myös huomioitava, että tukiaseman sijoittaminen toimistotarvikevarastoon ei ole suositeltavaa papeririisien aiheuttaman kovahkon attenuaation takia.

### **3.6 Langattoman siirtotien suojaus**

Kuten on pohjustettu aiemmissa osissa, tavanomainen WLAN- antennimoduuli on ympärisäteilevä, eikä suinkaan tiukasti suunnattu lähetyks lähettäjän ja vastaanottajan välillä. Tämä tarkoittaa mm. sitä, että lähetystä kykenee tarkkailemaan ja analysoidaan muutkin tahot kuin olisi tarkoitus. Lisäksi suojaamaton, täysin oletusasetuksilla toimiva tukiasema, mahdollistaa hallitsemattoman pääsyn lähiverkkoon, mihin se on välittömästi liitetty kaikille niille, jotka kuulevat sen lähettämän SSID:n.

Käänteisesti ajateltuna langattoman verkon suurin etu, että sitä on vaivaton käyttää yhteysväylänä joko MAN-verkkoon, työryhmään tai molempiin, kääntyy sitä vastaan, jos tilannetta ryhdytään tarkastelemaan tietoturvallisuuden kannalta. Täytyy pitää kuitenkin mielessä, että otollisilla hetkillä 802.11g- standardin tukiasema saattaa lähettää kuuluvaa signaalia yli 70 metrin päähän. Se tarkoittaa useimmissa tapauksissa signaalin päätyvän lähiverkon tarkoitettun käyttöympäristön ulkopuolelle, joka mahdollistaa verkon väärinkäytön.

Seuraavassa on listattu neljä eri suhteessa tehokasta tapaa rajata langattoman verkon käyttäjäkunta täysin halutun kaltaiseksi. Näitä yhdistelemällä tuotetaan halutun kaltaisen tietoturvan taso. Pääsääntöisesti, mitä enemmän verkon ylläpito tuottaa tietoturvallisuuteen kantaaottavia moduuleja, sitä epäkäytettävämmäksi järjestelmä muuttuu.

*Tukiasemaan MAC-suodatus.* Vain ennalta määritetyt MAC-osoitteet saavat asiakkuuden langattomaan verkkoon. Tämä on varsin epäkäytännöllinen toimipisteissä,

joissa on paljon satunnaisesti vaihtuvia vieraita päätelaitteineen. Yhdistettynä WPA2 -salaukseen se on tehokkain käytössä oleva tapa rajata vain haluttu käyttäjäryhmä.

*Kryptaus.* Käytännössä kaikissa 802.11 standardin kategorioissa toimivat WEP ja WPA -tuoteperheet. Kryptausta on käsitelty seuraavassa luvussa hieman kattavammin. Karkeasti metodi toimii siten, että tukiasema salaa tiedon käyttäen salausavainta (cipheria) ja vastaanottaja saa tiedon purettua tietämällä oikean salausavaimen. Tämä salausavain syötetään ja paritetaan SSID:hen samalla hetkellä, kun yritetään liittyä asiakkaaksi langattomaan lähiverkkoon. Jos syötetty avain on väärin, niin päätelaitteella on vajaa tai puuttuva liitettävyys.

*Salasana ja käyttäjänimi.* Suositeltavaa on myös vaihtaa tukiaseman hallinnointiin tarvittavat pääkäyttäjän nimi ja salasana. Aina, jos tukiasemaan pääsee fyysisesti käsi, on sen hallinnoiman langattoman lähiverkon tietoturva uhattuna.

*Autentikaatio.* Käyttäjän autentikaation voi toteuttaa eri tavoin, mm. liittämällä pääte-laite AD-palvelimeen, tai syöttämällä käyttäjänimi sekä salasana selaimen ensimmäisen käynnistytksen yhteydessä. OpenSparkissa on käytössä ainoastaan viimeisenä mainittu metodi todentaa käyttäjä. Metodissa on sekä hyvät että todella huonot puolensa.

Useimpien valmistajien lippulaivamalleissa pääsee asetuksista hienosäätämään mm. syöttövirtaa antenniin, millä saadaan rajattua kantomatkaa halutun kaltaiseksi. Tämä metodi kuitenkin vähentää kantomatkan lisäksi myös signaalin rakenteiden läpäisykykyä, joten pääsääntöisesti ei ole järkevä idea kuristaa antennin tehon syöttöä.

## **WEP ja WPA**

WEP ja WPA ovat kaksi keskeistä metodia, jotka tuottavat sekä autentikaation että salauksen langattomaan lähiverkkoon. Molempia metodeita pystytään käyttämään kaikissa neljässä 802.11 versioissa. WEP- salaus on kahdesta vanhempi ja haavoittuvaisempi salauksen murtamiseen, mutta vanhemmissa päätelaitteissa ja ohjelmistoissa on parempi tuki siihen. WPA ja siitä kehitetty uudempi versio WPA2 on moderni ja käytännössä katsoen murtamaton salaus. Vaikka WPA-salauksesta kaiken aikaa löy-



detään uusia haavoittuvaisuuksia. Siihen kuitenkin vielä ole netistä suoraan ladattavia työkaluja, jotka lähes automaattisesti pystyisivät sitä purkamaan.

Wired Equivalent Privacya käytetään suojaamaan langatonta siirtotietä salakuuntelulta. Toissijainen funktio WEP-salauksessa on estää valtuuttamattomat liittynät verkon tukiasemaan. Koko WEP-salaus pohjautuu salaiseen avaimen päätelaitteen ja tukiaseman välillä. WEP käyttää RC4-salausalgoritmia. Se pohjautuu näennäislukugeneraattoriin, joka tuottaa mahdollisimman isoja satunnaislukuja (Borisov, Goldberg & Wagner, [viitattu 9.2.2010]). Sen tuottama luku on vuon salausavain. Salausavain on joko ASCII-tai heksamuodossa, ja se on määrämittainen, joko 64, 128 tai 256 bittiä. Kuten aikaisemmin todettiin, sen ainoa hyvä puoli on yhteensopivuus ensimmäisen sukupolven verkkolaitteiden kanssa. Jos on mahdollista, niin aina tulisi valikoida käyttöön WPA tai WPA2.

WPA:sta eli Wi-Fi Protected Accessista on saatavilla kaksi eri versiota, WPA ja WPA2. Pääsääntöinen ero näissä kahdessa on salausmetodi, jolla radioteitse liikutettava data salataan. Uudempi WPA2 käyttää AES- metodia, joka on käytännössä katsoen murtamaton nykyään. Vanhempi WPA turvautuu vaihtuvan avaimen eheyden protokollaan eli TKIP:seen (Temporal Key Integrity Protocol), joka on myös paljon turvallisempi metodi suojata siirtotie kuin WEP.

Vaikka TKIP on mahdollista purkaa noin 20 minuutissa suuria paketti-injektioita käyttäen, WPA-salauksen murtaminen edellyttää kuitenkin paljon suurempaa tietotaitoa kuin esim. WEP-salauksen. TKIP on myös mahdollista saada toimimaan vanhemmissa WLAN- adaptereissa firmwarepäivityksen jälkeen. Joissakin lähteissä WPA2-protokollaa kutsutaan sen IEEE-työnimellä eli 802.11i:ksi. Joskus myös tiettyjen valmistajien firmwareissa WPA- ja WPA2-salauksia kutsutaan joko WPA personaliksi tai WPA-psk:si (pre-shared key). Termi pre-shared viittaa vain salausavaimeen, joka on sama tukiasemalla ja päätelaitteella. Täten sitä ei koskaan lähetetä.

Wi-Fi- allianssi on määrittänyt seuraavat laajennukset WPA- ja WPA2- salauksiin. Koko laajennusperhettä käsitellään yleensä monissa lähteissä vain akronyymina EAP.

EAP-laajennuksessa on mahdollista tuottaa käyttäjäautentikaatio esim. SIM-kortilla (EAP-sim). Langattoman siirtotien suojaus olisi aihepiirinä kokonaisen opinnäytetyön laajuinen kokonaisuus. WEP ja WPA sekä niiden laajennukset mainitaan tässä pinta-puolisesti lähinnä kuriositeetin takia.

Lemminkäisenkadun toimipisteen SparkNetissä ei ole käytössä minkäänlaista salausta vaan haluttu käyttäjäkunta rajataan selainpohjaisella autentikaatiolla.

#### **4 LEMMINKÄISENKADUN TOIMIPISTEEN ESITTELY (Salattu)**

#### **5 LANGATTOMAN VERKON DOKUMENTOINTI (Salattu)**

## 6 POHDINTA

Työni koostuu teoreettisesta viitekehystä, jossa on mm. yleiskatsaus WLAN- teknologioista, lähiverkkotopologioista sekä tietoliikenneprotokollista. Mahdollinen käyttötarkoitus teoreettiselle viitekehykselle on esimerkiksi luentomateriaali tietoliikenteen perusteisiin. Lähdemateriaaleissa esiintyvät julkaisut olivat myös varsin kelvollista materiaalia tietoliikenteen opintoihin. Ongelmana kattavan teoreettisen materiaalin luomisessa oli pääsääntöisesti suomen- ja englanninkielisen termistön yhteensovittaminen niin, että se on yksiselitteistä ja yleisesti hyväksyttyä kirjoitusasua. Mukaan liitetty sanasto toivottavasti edesauttaa materiaalin ymmärrettävyyttä.

Empiriaosuus opinnäytetyöstä haluttiin salata tilaajatahon toimesta. Tämä on varsin yleistä, kun kyseessä on verkkoa käsittelevät dokumentaatiot. Syykin tähän on varsin looginen, sillä dokumentaatiosta voidaan koostaa melko helposti ”hakkerimanuaali”, koska kattava verkkodokumentaatio ottaa myös kantaa verkon ongelmakohtiin ja kippusteisiin parannusehdotusten nimissä. Nämä mainitut seikat voidaan kääntää helposti haavoittuvaisuuskartoitukseen, joka osaltaan altistaa verkon pahantahtoisille hyökkäyksille ja väärinkäytölle.

Tuleville opiskelijoille Lemminkäisenkadun toimipisteen lähiverkko tuottaa taatusti mielenkiintoisia aiheita opinnäytetyötarpeisiin. Mahdollisuuksia on monia, kuten dokumentoiminen, mahdollisten parannusehdotusten laatiminen tai jopa WLAN-verkon kuuluvuusaluekartan luominen.

## LÄHTEET

- ATIS 2007. *ATIS Telecom glossary* [online, viitattu 29.1.2010] Saatavilla www-muodossa:  
<URL: <http://www.atis.org/glossary/definition.aspx?id=6101>>.
- Borisov, Nikita, Goldberg, Ian & Wagner, David 2001. *Security of the WEP algorithm* [online, viitattu 9.2.2010] Saatavilla www-muodossa :  
<URL: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>>.
- Briere, Danny, Ferris, Edvard & Hurley, Pat 2008. *Wireless home networking for dummies third ed.* Indianapolis:Wiley publishing inc.
- EventHelix.com 2000-2009. *Reliability and availability basics* [online, viitattu 12.4.2010] Saatavilla www-muodossa:  
<URL:[http://www.eventhelix.com/RealtimeMantra/FaultHandling/reliability\\_availability\\_basics.htm](http://www.eventhelix.com/RealtimeMantra/FaultHandling/reliability_availability_basics.htm)>.
- Georgia Tech, the college of computing 2010. *Questionnaire Design* [online, viitattu 21.1.2010] Saatavilla www-muodossa:  
<URL: [http://www.cc.gatech.edu/classes/cs6751\\_97\\_winter/Topics/questionnaire\\_design/](http://www.cc.gatech.edu/classes/cs6751_97_winter/Topics/questionnaire_design/)>.
- Knowledgerush 2009. *ALOHA*net [online: viitattu 29.1.2010] Saatavilla www-muodossa:  
<URL: <http://www.knowledgerush.com/kr/encyclopedia/ALOHA.net/>>.
- Masterplanet Oy 2010. *MP-Masterplanet* [online, viitattu 18.4.2010] Saatavilla www-muodossa:  
<URL: <http://www.masterplanet.fi/index.php>>.
- Mitchell, Bradley 2010. *LAN – Local Area Network* [online, viitattu 28.1.2010] Saatavilla www-muodossa:  
<URL: [http://compnetworking.about.com/cs/lanvlanwan/g/bldef\\_lan.htm](http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm)>.
- Networktutorials 2007. *An overview of computer network topology* [online, viitattu 28.1.2010] Saatavilla www-muodossa:  
<URL: <http://www.networktutorials.info/topology.html>>.
- Ojanperä, Veijo 2004. *Nopeat laiteyhteydet langattomaksi* [online, viitattu 4.2.2010] Saatavilla www-muodossa  
<URL: <http://www.proessori.fi/es04/arkisto/uwb.html>>.
- Peterson L. Larry & Davie S. Bruce 2000. *Computer networks, a systems approach second ed.* San Diego: Academic press.

- Petri, Daniel 2009. *Osi model concepts* [online, viitattu 25.2.2010] Saatavilla www-muodossa:  
<URL: [http://www.petri.co.il/osi\\_concepts.htm](http://www.petri.co.il/osi_concepts.htm)>.
- Pidgeon, Nick 2010. *How Ethernet works* [online, viitattu 25.2.2010] Saatavilla www-muodossa:  
<URL: <http://computer.howstuffworks.com/ethernet.htm>>.
- Puska, Matti 2005. *Langattomat lähiverkot*. Jyväskylä: Talentum media Oy.
- Protocols 2010. *TCP-IP Suite* [Online, viitattu 27.1.2010] Saatavilla www-muodossa:  
<URL: <http://www.protocols.com/pbook/tcpip2.htm#IP>>.
- Stallings, William 2007. *Data and computer communications, eight edition*. New Jersey: Pearson.
- StatPac Inc.2010. *Questionnaire design general considerations* [online, viitattu 21.1.2010] Saatavilla www-muodossa:  
<URL: <http://www.statpac.com/surveys/questionnaire-design.htm>>.
- Trendcomms 2010. *A Brief history of Ethernet* [online, viitattu 29.1.2010] Saatavilla www-muodossa:  
<URL:<http://www.trendcomms.com/multimedia/training/broadband%20networks/web/main/Ethernet/Theme/Chapter1/EnetBriefHistory.html>>.
- Tunturi Mopedit 2009. *Historiaa* [online, viitattu 18.4.2010] Saatavilla www-muodossa:  
<URL:<http://www.freewebs.com/pappamopedit/tietoatunturipyroyst.htm>>.
- Turku AMK 2008. *Sparknet* [online, viitattu 18.4.2010] Saatavilla www-muodossa:  
<URL:<http://www.turkuamk.fi/Public/default.aspx?uielements=1&nodeid=7993>>.
- Wikipedia 2010a. *Carrier grade* [online, viitattu 20.10.2010] Saatavilla www-muodossa:  
<URL: [http://en.wikipedia.org/wiki/Carrier\\_grade](http://en.wikipedia.org/wiki/Carrier_grade)>.
- Wikipedia 2010b. *Cisco Systems* [online, viitattu 20.10.2010] Saatavilla www-muodossa:  
<URL: [http://en.wikipedia.org/wiki/Cisco\\_Systems](http://en.wikipedia.org/wiki/Cisco_Systems)>.
- Wikipedia 2010c. *SparkNet* [online, viitattu 14.4.2010] Saatavilla www-muodossa:  
<URL:<http://fi.wikipedia.org/wiki/SparkNet>>.
- Wilson J. Mark 2008. *The ARRL handbook for radio communications. The comprehensive RF engineering reference* 85. ed. Newington: ARRL – the national association for amateur radio.

Wi Revolution 2008. *Is 802.11n too power-hungry for handsets?* [online, viitattu 3.2.2010] saatavilla www-muodossa:  
<URL: <http://www.wirevolution.com/2008/06/23/is-80211n-too-power-hungry-for-handsets/>>.

Wi-Fi Alliance 2009. *FAQs* [online, viitattu 3.2.2010] saatavilla www-muodossa:  
<URL: [http://www.wi-fi.org/knowledge\\_center\\_overview.php?type=2](http://www.wi-fi.org/knowledge_center_overview.php?type=2)>.

## LIITTEET

## LIITE 1/1(2)

### 1 SANASTO

|            |   |
|------------|---|
| 802.11x    | IEEE:n standardi langattomille WLAN-lähiverkoille.  |
| Ad-hoc     | Latinaa, tässä yhteydessä koneiden langaton yhteenliittymä, ei kaistaa ulos.                          |
| AMK        | Ammattikorkeakoulu  |
| BSS        | Tukiasemallinen verkko, liityntäpiste Basic service set   |
| CSMA/CA    | Carrier sense multiple access with collision avoidance. Langattoman siirtotien varausmetodi           |
| CSMA/CD    | Carrier sense multiple access with collision detection. Langallisen siirtotien varausmetodi           |
| DNS        | Internetin nimipalvelujärjestelmä. Muuntaa nimiä IP-osoitteiksi. Domain name system.                  |
| ESSID      | Yhteenliitettyjä BSS-verkkoja. Extended service set   |
| Ethernet   | Pakettipohjainen, maailman yleisin, lähiverkkoratkaisu  |
| FreeRADIUS | Maailman yleisin RADIUS-ohjelmisto. Avointa lähdekooda.   |
| FTP        | Tiedostonsiirtoprotokolla   |
| Ghz        | Gigahertsi, miljardi värähdystä sekunnissa  |
| http       | Hypertekstin siirtoprotokolla. Mm. www-palvelimet käyttävät tätä.                                     |
| IEEE       | Institute of Electrical and Electronics Engineers. Voitto tavoittelematon standardisointiorganisaatio |
| IP         | Internet protocol. Ethernetpakettien toimittaminen.   |
| ISO        | Kansainvälinen standardisimisjärjestö   |
| LAN        | Lähiverkko. Local area network  |
| MAC        | Verkon päätelaitteita yksilöivä osoite. Valmistajan määrittelemä ja uniikki maailman laajuisesti.     |
| NAT        | Osoitteenmuutos. Yhden julkisen IP-osoitteen takana voi olla useita erillisiä päätelaitteita          |
| Mhz        | Megahertsi, miljoona värähdystä sekunnissa  |
| OSI-malli  | Tiedonsiirtoprotokollien yhdistelmä seitsemässä kerroksessa. Teoreettinen, ei sellaisenaan käytössä   |
| PoE        | Sähkön siirto ethernetkaapelia pitkin. Power over ethernet.   |
| RJ-45      | Liitintyyppi kierrettyyn parikaapeliin. Yleisesti käytössä ethernetsovelluksissa.                     |
| SMTP       | Käytetään sähköpostiviestien välittämiseen. Käyttää porttia 25  |

|         |  |
|---------|--|
| SSID    | Tukiaseman nimi, jota se lähettää. Yksilöivä   |
| TCP     | Vuonhallintaprotokolla. Transmission control protocol. Yhdistetään IP-protokollaan.                    |
| UWB     | Radioteknologian sovelluskohde lyhyen kantaman nopeaan tiedonsiirtoon.                                 |
| WAN     | Laajan alueen verkko, joka peittää laajoja maantieteellisiä alueita                                    |
| Web 2.0 | Pääsääntöisesti kaupallinen nimitys käyttäjien luomaa sisältöä koostaviin sivustoihin. Esim. Wikipedia |
| WEP     | Ensimmäinen langattoman siirtotien suojaukseen kehitetty salausmenetelmä.                              |
| WiFi    | Wi-Fi alliansin tavaramerkki, joka takaa kaikkien Wi-Fi laitteiden yhteensopivuuden. Wireless Fidelity |
| WLAN    | Langaton lähiverkko. Wireless local area network   |
| WPA     | WEP-salausta uudempi ja varmempi metodi suojata langaton siirtotie.                                    |